ABSTRACT OF THE DISCLOSURE

A system that produces one or more non-repeating randomizer sequences of up to 2^m-1 or more m-bit symbols includes a randomizer circuit that is set up in accordance with a polynomial with primitive elements of GF(2^m) as coefficients. The system combines the randomizer sequence with all the symbols of ECC code words that are encoded using a BCH code over GF(2^m) to produce a randomized code word. The particular primitive elements used and/or an initial state of one or more registers in the system specifies the particular sequence produced by the system. The initial state of each of the one or more registers is a selected one of the 2^m-1 elements of GF(2^m), and thus, 2^m-1 different sequences may be produced by selecting a different initial state for a given one of the registers. If the coefficients are also selected from, for example, a set of "p" possible values, the system produces p*(2^m-1) different sequences. The system may thus be used to encrypt the ECC code word by associating the code word with a particular selected initial state and/or coefficient. The coefficients may be selected to produce randomizer sequences that are predetermined minimum distances away from both the ECC code words.